MoGua

服务通 iet2sbkj.APK 分析报告

APP名称:	服务通

包名:	pak4c0vnfr.sg7ifglp4w.df89v7mx6w
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: pak4c0vnfr.sg7ifglp4w.df89v7mx6w (1).apk
文件大小: 23.66MB

MD5值: 84d20da91eb5e1ff836da57ed9f2ea36
SHA1值: f9b41bfbd310cbb671973decb789c2b9cbabbf7b
SHA256值: ee61d2f9ec888e03f74250cc5cc0fd58c30d2d4a677c97e943f96fd0b115c853

APP 信息

App名称: 服务通
包名: pak4c0vnfr.sg7ifglp4w.df89v7mx6w
主活动Activity: pak4c0vnfr.sg7ifglp4w.df89v7mx6w.MainActivity
安卓版本名称: iet2sbkj
安卓版本: 43271650

域名线索

URL线索

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-02 11:33:24+00:00
有效期至: 2125-05-09 11:33:24+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0xd8e63636da57dfd1
哈希算法: sha384
md5值: e83b445d9767b9f1269c10d4d611d3d6
sha1值: 17522e08232cbbad1f87b4bc428ea1d0ff6656a5
sha256值: bb134977bd45324e732a894173512ce28ce0ed5eff8108cedbcc2110503a790d
sha512值: ec339f28b3dd903110a1e190fb2f2f751981440fa3e7b05be3170714bcda5652d0410fb81a7aa2e91995794b764cf186642de9a54ac1f735b693b514cb1e01f6
公钥算法: rsa
密钥长度: 2048
指纹: 9e112088607c1edeb45a2bdb69401fbc11d993514dba769903aa708fe8053681

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

	是否		

向手机申请的权限	危险	类型	详细情况
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕

pak4c0vnfr.sg7ifglp4w.df89v7mx6w.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
pak4c0vnfr.sg7ifglp4w.df89v7mx6w.MainActivity	Schemes: begatljh://,

---